

ORIGINAL

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----x

UNITED STATES OF AMERICA

- v. -

JOHN DOE 1,  
JOHN DOE 2,  
JOHN DOE 3,  
JOHN DOE 4,  
JOHN DOE 5,  
JOHN DOE 6, and  
JOHN DOE 7,

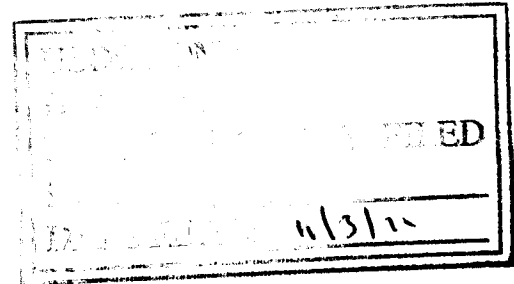
Defendants.

-----x

SEALED

POST-INDICTMENT  
PROTECTIVE ORDER,  
PURSUANT TO 21 U.S.C. §  
853(e)(1)(A) &  
18 U.S.C. § 1956(b)(4)

S2 11 Cr. 878



WHEREAS, on or about November 1, 2011, by and through  
PREET BHARARA, United States Attorney for the Southern District  
of New York, the Government submitted a sealed application of  
Assistant United States Attorney James Pastore, together with  
the sealed declaration of Special Agent Sean Zadig of the  
National Aeronautics and Space Administration ("NASA"), seeking  
certain relief pursuant to Title 21, United States Code, Section  
853(e)(1)(A) and Title 18, United States Code, Section  
1956(b)(4);

WHEREAS, a Grand Jury sitting in this District has  
returned an Indictment charging JOHN DOE 1, JOHN DOE 2, JOHN DOE  
3, JOHN DOE 4, JOHN DOE 5, JOHN DOE 6, and JOHN DOE 7, the  
defendants, with wire fraud and conspiracy to commit wire fraud,  
in violation of Title 18, United States Code, Sections 1343 and

1349, computer intrusion and conspiracy to commit computer intrusion in violation of Title 18, United States Code, Section 1030, and money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957;

WHEREAS, the Indictment has specifically alleged that the following property is subject to criminal forfeiture, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982, and 1030(i), and Title 28, United States Code, Section 2461:

1. The defendants' interests in all computers and computer peripherals:

a. associated with IP addresses 85.255.112.0 through 85.255.127.255; 67.210.0.0 through 67.210.15.255; 93.188.160.0 through 93.188.167.255; 77.67.83.0 through 77.67.83.255; 213.109.64.0 through 213.109.79.255; 64.28.176.0 through 64.28.191.255; 69.197.132.58; 72.233.76.82; 174.123.205.190; 174.133.7.122; 184.82.214.2; 216.127.191.66; 64.20.51.2; 65.60.9.234; 65.60.9.235; 65.60.9.236; 65.60.9.237; 65.60.9.238; 66.152.177.58; 72.18.192.58; 72.18.192.59; 72.18.192.60; 72.18.192.61; 72.233.76.66; 72.233.76.67; 72.233.76.68; 72.233.76.69; 72.233.76.70; 65.254.36.122; 65.254.50.10; 72.9.238.202; 75.127.76.194; 207.210.119.170; 216.180.243.10; 64.111.197.186; 66.230.167.218; and 69.93.95.234 (the "Target IP Addresses");

- b. located at Pilosoft in New York, New York  
(the "Manhattan Data Center");
- c. located at ColoSecure in Chicago, Illinois,  
(the "Chicago Data Center");
- d. located at ThePlanet in Houston, Texas;
- e. located at Multacom Corporation in Canyon  
County, California;
- f. located at Layered Technologies in Plano,  
Texas;
- g. located at Network Operations Center, Inc.  
in Scranton, Pennsylvania;
- h. located at Wholesale Internet in Kansas  
City, Missouri;
- i. located at SingleHop in Chicago, Illinois;
- j. located at PremiaNet in Las Vegas, Nevada;
- k. located at Interserver in Secaucus, New  
Jersey;
- l. located at ISPrime, LLC, in Weehawken, New  
Jersey; and
- m. located at Global Net Access LLC, in  
Atlanta, Georgia; and

2. The defendants' interests in the TARGET IP ADDRESSES (collectively with item (1) set forth above, the "Forfeitable Property").

WHEREAS, the Court finds that there is probable cause to believe that in the event that the defendants are convicted of the charges in the Indictment, the Forfeitable Property will be subject to criminal forfeiture;

WHEREAS, the Court further finds that a protective order is necessary to preserve the Forfeitable Property for forfeiture, and to prevent harm to certain individuals whose computers have been infected with malicious software;

**IT IS HEREBY ORDERED** that:

1. JOHN DOE 1, JOHN DOE 2, JOHN DOE 3, JOHN DOE 4, JOHN DOE 5, JOHN DOE 6, and JOHN DOE 7, the defendants; and

2. All attorneys and other persons and entities acting for or in concert with the above-named defendants, businesses and/or entities having actual knowledge of this Order;

Shall not take any action prohibited by this Order;

**IT IS FURTHER ORDERED** that:

3. the defendants, their attorneys, agents, employees and anyone acting on their behalf, and all persons or entities acting in concert or participation with any of the above, and all persons and entities having actual knowledge of this Order, shall not, directly or indirectly, transfer, sell, assign, pledge, hypothecate, encumber, or dispose of in any manner; cause to be transferred, sold, assigned, pledged,

hypothecated, encumbered, disposed of in any manner; or take, or cause to be taken, any action that would have the effect of depreciating, damaging, or in any way diminishing the value of property or other interests belonging to, or owed to, or controlled in whole or in part by the defendants, which property or other interests are subject to forfeiture, including but not limited to the Forfeitable Property;

**IT IS FURTHER ORDERED** that:

4. the United States Attorney's Office for the Southern District of New York, in its discretion, is authorized to direct the release of the Forfeitable Property;

5. The institutions listed in this Order where the defendants maintained assets may contact the following Assistant United States Attorneys to clarify the scope of the Order: Assistant United States Attorneys Alexander J. Wilson, James Pastore, and Sarah Lai, Telephone Number (212) 637-1583. Those institutions will not be deemed in violation of this Order for any transactions undertaken upon written authorization made by any one of the aforementioned Assistant United States Attorneys. Each fourteen-day period beginning November 8, 2011 and ending March 22, 2012, the United States Attorney's Office shall file with the Court a report concerning any such written authorizations issued during the preceding 14 days.

IT IS FURTHER ORDERED that:

6. Internet Systems Consortium ("ISC") is appointed as a receiver to take any and all steps reasonably necessary to install, monitor, and administer one or more Domain Name System ("DNS") servers (the "Replacement DNS Servers") that will replace certain DNS servers (the "Rogue DNS Servers") which are currently operated and/or controlled by the defendants, and which are located at the Manhattan Data Center and at the Chicago Data Center;

7. ISC shall operate the Replacement DNS Servers for a period of 120 days, beginning on or about November 8, 2011 and ending on or about March 8, 2012.

8. ISC shall take steps to identify computers that are infected with malicious DNS changer software (the "DNS Changer Malware") by collecting the IP addresses that query the Replacement DNS Servers and the date and time of such requests, but shall not collect any content associated with such requests;

9. ISC is authorized under the guidance of the FBI to provide remediation details to industry channels approved by the FBI;

10. On or before January 23, 2012, ISC shall submit a report to the Court regarding its operation of the Replacement DNS Servers, which will include an estimate of the number of

victims identified by ISC through January 8, 2012 and such other information as ordered by the Court.

11. On or before March 22, 2012, ISC shall submit a final report to the Court regarding the number of victims identified by ISC and such other information as ordered by the Court.

12. Each Internet Service Provider ("ISP") receiving notice of this Order shall refrain from taking any steps at the request of the defendants and/or their co-conspirators or their agents that would cause Internet traffic to be re-routed away from the Replacement DNS Servers, including, but not limited to, refraining from, in response to such a request, announcing new routes for any IP address that is identified by the FBI as being associated with the defendants or their co-conspirators, and shall announce such routes for such IP addresses as directed by the FBI in order to ensure that DNS queries reach the Replacement DNS Servers;

13. Each Regional Internet Registry ("RIR") receiving notice of this Order shall take all steps necessary to prevent and prohibit the defendants and their co-conspirators from:

a. effectuating any change of control over the current registration accounts for the Target IP Addresses;

b. making any changes to the registration records for the Target IP Addresses unless prior authorization

is received from the FBI, or the United States Attorney's Office for the Southern District of New York ("USAO-SDNY"); or

c. directly or indirectly attempting to transfer the Target IP Addresses to any other individuals or entities, except as approved by the FBI, or the USAO-SDNY.

14. Each data center receiving notice of this Order shall take all steps reasonably necessary to prevent the removal, deletion, or destruction of computers identified by the FBI as computers in which the defendants or their co-conspirators currently maintain any interest - including, but not limited to, disabling Internet access for such computers - in order to preserve those computers for forfeiture, provided, however, that this Order applies only to the portion(s) of the computers in which the defendants or their co-conspirators have an interest.

**IT IS FURTHER ORDERED** that:

15. this Protective Order shall be binding upon the defendants, their attorneys, agents, and employees, and all persons in active concert or participation with any of the above, all institutions described herein, or any other person having actual knowledge of this Order, and that this Order shall remain in effect until further order of this Court;



IT IS FURTHER ORDERED that:


16. service of a copy of this Order shall be made on the defendants' attorneys by regular mail;

IT IS HEREBY FINALLY ORDERED that:

17. this Order shall remain under seal and shall be captioned as *United States v. John Doe 1, et. al*, until the unsealing of the Indictment, S2 11 Cr. 878, or further Order of this Court, except that the United States Attorney's Office for the Southern District of New York may obtain and disseminate copies of this Order as necessary to execute this Order.

Dated: New York, New York  
November 3, 2011

SO ORDERED:

  
HONORABLE WILLIAM H. PAULY III  
UNITED STATES DISTRICT JUDGE  
SOUTHERN DISTRICT OF NEW YORK